Safety Evaluation Approach with Security Controls for Safety I&C Systems on Nuclear Power Plants

D.H. Kim[a*], S.Y. Jeong[a], Y.M. Kim[a], M.S. Lee[b], T.H. Kim[b]and H. S. Park[a]
[a]*Korea Institute of Nuclear Safety, 62 Gwahak-ro, Yuseong-gu, Daejeon, Korea, 305-338*
[b]*Formal Works Inc., 110 Banpo-r, Seocho-gu, Seoul, Korea, 137-872*
[*]*Corresponding author: k730kdh@kins.re.kr*

1. Introduction

As the use of digital technology is increasing in I&C nuclear I&C systems, the possibility of cyber attacks to the systems has been increased. The digital I&C systems must be adequately protected from cyber attacks that would adversely impact the safety of the system. But, where cyber security features need to be implemented on safety-related digital I&C systems, adequate measures should be taken to ensure that these features do not adversely affect the ability of a system to perform its safety functions[1].

This paper addresses concepts of safety and security and relations between them for assessing effects of security features in safety systems. Also, evaluation approach for avoiding confliction with safety requirements and cyber security features which may be adopted in safety-related digital I&C system will be described.

2. Background

2.1 Safety and Security

The term safety and security are used with the same sense in some area and they have different meaning in other fields. In the field of nuclear energy, safety and security have the same purpose to respond to risk that can occur in the system, but they treat different object that generates the risk to the system. The document of IAEA Safety Glossary defines the concept of safety and security as shown in Table 1.

Table 1. IAEA Safety Glossary − Safety, Security[2]

(Nuclear) Safety: The achievement of proper operating conditions, prevention of accidents or mitigation of accident consequences, resulting in the protections of workers, the public and the environment from undue radiation hazards.
(Nuclear) Security: The prevention and detection of, and response to theft, sabotage, unauthorized access, illegal transfer or other malicious acts involving nuclear material, other radioactive substances or their associated facilities.

Considering of the definition, safety and security are all talking about responding to risk. However, they are different since they have different origins to generate the risk. Safety considers the risk occurred from unintended events or system's problems. And security considers the risk resulted from the malicious behaviors.

In terms of techniques for safety and security, they can be classified into two techniques, such as techniques to analyze risks and techniques to respond to risk. Techniques to analyze the risk can be used for both safety and security. However, there are some portions that may result in a conflict between safety and security about the technique to respond to risk. Because they have a different origin of risk with similarity corresponding to the technique to respond to risk.

2.2 Security Control and MMIS(Man Machine Interface System)

U.S. NRC R.G. 5.71 provides a list of security controls should be applied to control system of Nuclear Power Plant[3]. Security controls can improve the system security, but they can affect the safety of MMIS. Because security and safety have different properties, even they have some common characteristics. Unlike the case of safety, security controls impose partial constraints to prevent malicious access and behavior from a user or an attacker. The constraints may affect the safety of the system or the usability of operators. Therefore, in order to apply security controls to the system, it should be considered the relevance between safety requirements and the effects of security control in MMIS.

2.3 Safety Requirement and MMIS

The safety requirements are needed to evaluate impact of security controls on the safety of MMIS. Safety requirements corresponding to specific evaluation cases are identified in safety-related standard documents. Especially, essential information that must be included in the safety requirements is described in the IEC 61513 "6. System Safety life Cycle - 6.2 Requirements"[4]. In this paper, the requirement items that are defined on this IEC standard are used to develop evaluation models.

3. Safety Effects Evaluation Model of Security Controls

3.1 Safety-Security Life cycle Model

In order to develop safety and security evaluation model in I&C systems, activities including in conventional method should be considered and required the equivalent quality in spite of existence of security controls. The strategy to evaluate safety effects of security control is that safety is prior to security in case of confliction between safety and security.

We propose the safety-security life cycle model which integrates requirements for safety and security. Fig. 1 shows the proposed safety-security life cycle model. This model identifies the confliction between activities for safety and security according to software life cycle. In the concept phase, hazard for safety and security is independently evaluated of each other. In the requirement phase, requirements for safety and security are independently identified based on evaluation results defined in the concept phase. These identified requirements are reviewed and modified if there is the confliction. After the requirement phase, requirements should be modified by the method defined in section 3.2.

3.2 Confliction Avoidance Method

In the safety-security life cycle model, it is important to avoid the confliction between requirements for safety and security. Fig. 2 shows the confliction avoidance method. The main concept of the proposed confliction avoidance method is to satisfy the safety requirement primarily and to modify the security requirement to avoid the confliction. If the confliction between safety requirement and security control is identified, the security requirement is discarded or replaced by an alternative requirement. The alternative requirement should be reviewed whether the security is ensured before the alteration of requirement.

4. Evaluation Results

In this section, we provide evaluation results for the safety effect in I&C system with security control. The safety effect is evaluated by 20 safety requirement items included in the IEC 61513[4]. U.S. NRC R.G. 5.71 provides security control items which are 147 items, and they are classified by the technical, operational, and management controls. If the safety requirement is adversely affected by the security control requirement, it is defined as 'confliction.' Table 2 summarizes the safety effect evaluation with security controls through examples of the representative confliction cases. As results of the evaluation, many of items for technical security control are expected to conflict with the safety requirements. The safety effect with operational and management security control is relatively less compared to that of technical control.

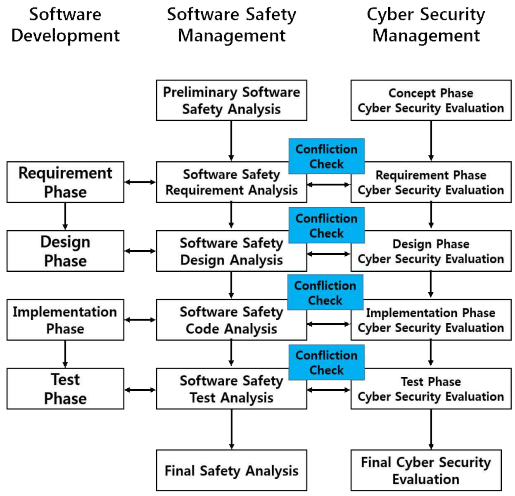

Fig. 1. Safety-security life cycle model

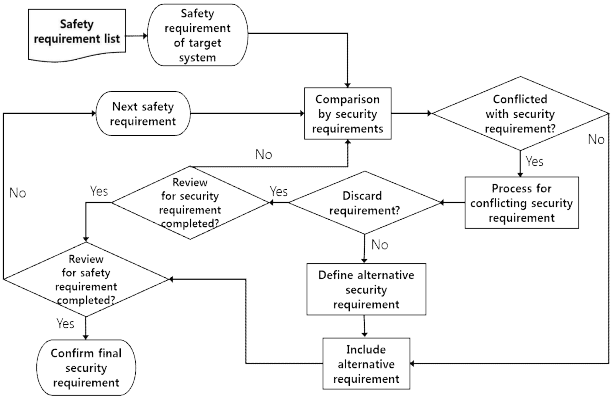

Fig. 2. Confliction avoidance method

Table 2. Safety effect with security control (Example)

Safety requirements	Confliction	Comments
Performance (e.g., accuracy and response times)	T,O, M	• Security control items such as access control can affect accuracy and response time. • Applying real-time malicious code detection mechanism can conflict in the safety system. • Risk mitigation technique can affect response time. etc.
Deterministic behavior (consistent performance)	T,M	• Many kinds of technical security controls, such as Information, flow enforcement access control, can disturb the consistent performance. etc. • Malicious code

Safety requirements	Confl iction	Comments
		protection can affect the consistent performance due to the non optimized technique. etc.
Sufficiently early detection of error and failure	T	• The performance of error and failure detection system to maintain safety system availability can be degraded due to some security control requirements. etc.
System design facilitating maintenance	T	• Security control such as access enforcement and least privilege can disturb easy maintenance such as failure detection, replacement, reconfiguration. process

**T: technical controls, O: operational controls, M: management controls*

5. Conclusions

In this paper, safety-security life cycle model based confliction avoidance method was proposed to evaluate the effects when the cyber security control features are implemented in the safety I&C system. Also, safety effect evaluation results using the proposed evaluation method were described. In case of technical security controls, many of them are expected to conflict with safety requirements, otherwise operational and managerial controls are not relatively.

Safety measures and cyber security measures for nuclear power plants should be implemented not to conflict with one another. Where safety function and security features are both required within the systems, and also where security features are implemented within safety systems, they should be justified.

We expect that the results of this study can help evaluating and justifying the cyber security features which need to be implemented in digital I&C systems.

Acknowledgements

This work was supported by the Nuclear Safety Research Program through the Korea Foundation Of Nuclear Safety(KOFONS), granted financial resource from the Nuclear Safety and Security Commission(NSSC), Republic of Korea (No. 1305003-0315-SB130).

REFERENCES

[1] MDEP, DICWG No8, Common Position on the Impact of Cyber Security Features on Digital I&C Safety Systems, 2012
[2] IAEA, Safety glossary: terminology used in nuclear safety and radiation protection, Ref. STI/PUB/1290, 2007 ed., 2007.
[3] NRC Regulatory Guide 5.71, Cyber Security Program for Nuclear Facilities, 2010
[4] IEC 61513, Nuclear power plants - Instrumentation and control important to safety general requirements for systems, 2011